

FIG. 1  
(Prior Art)

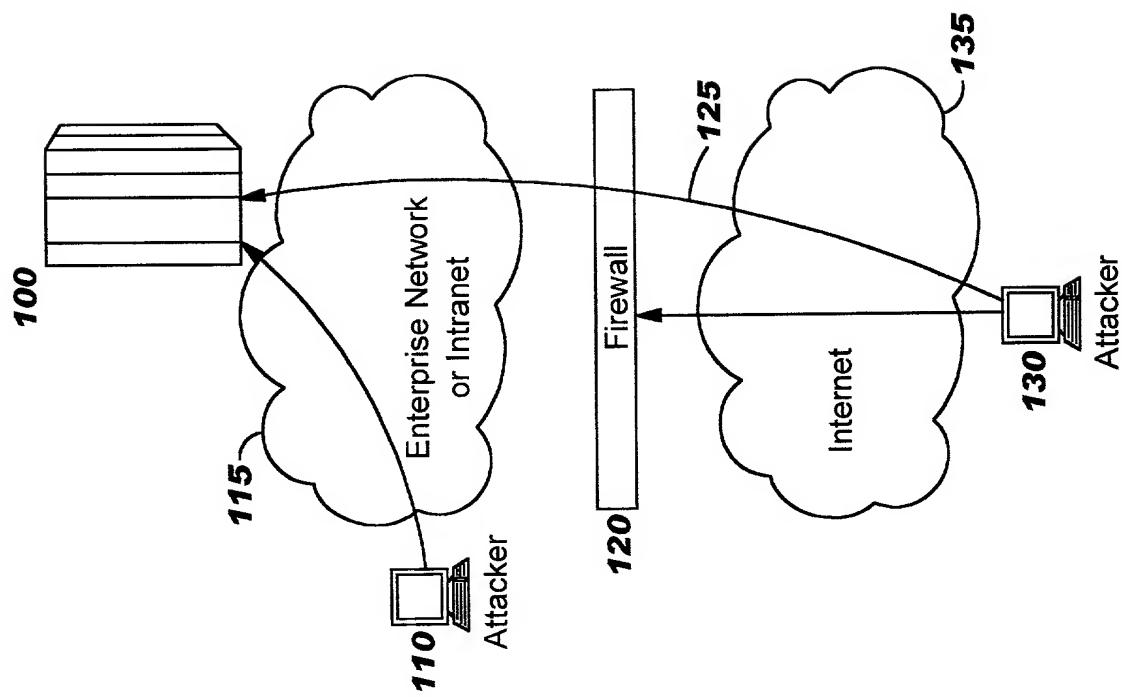


FIG. 2  
(Prior Art)

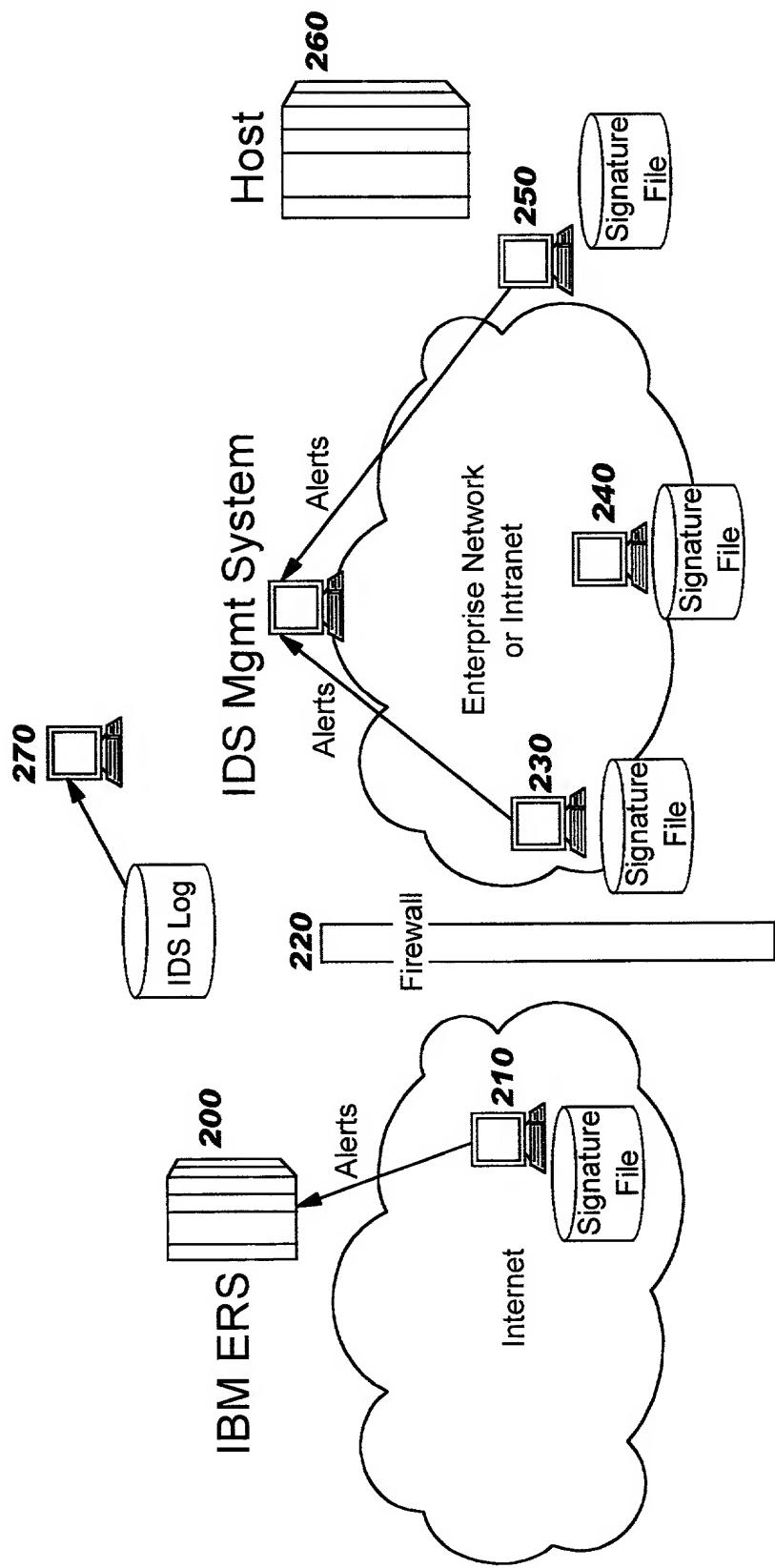


FIG. 3

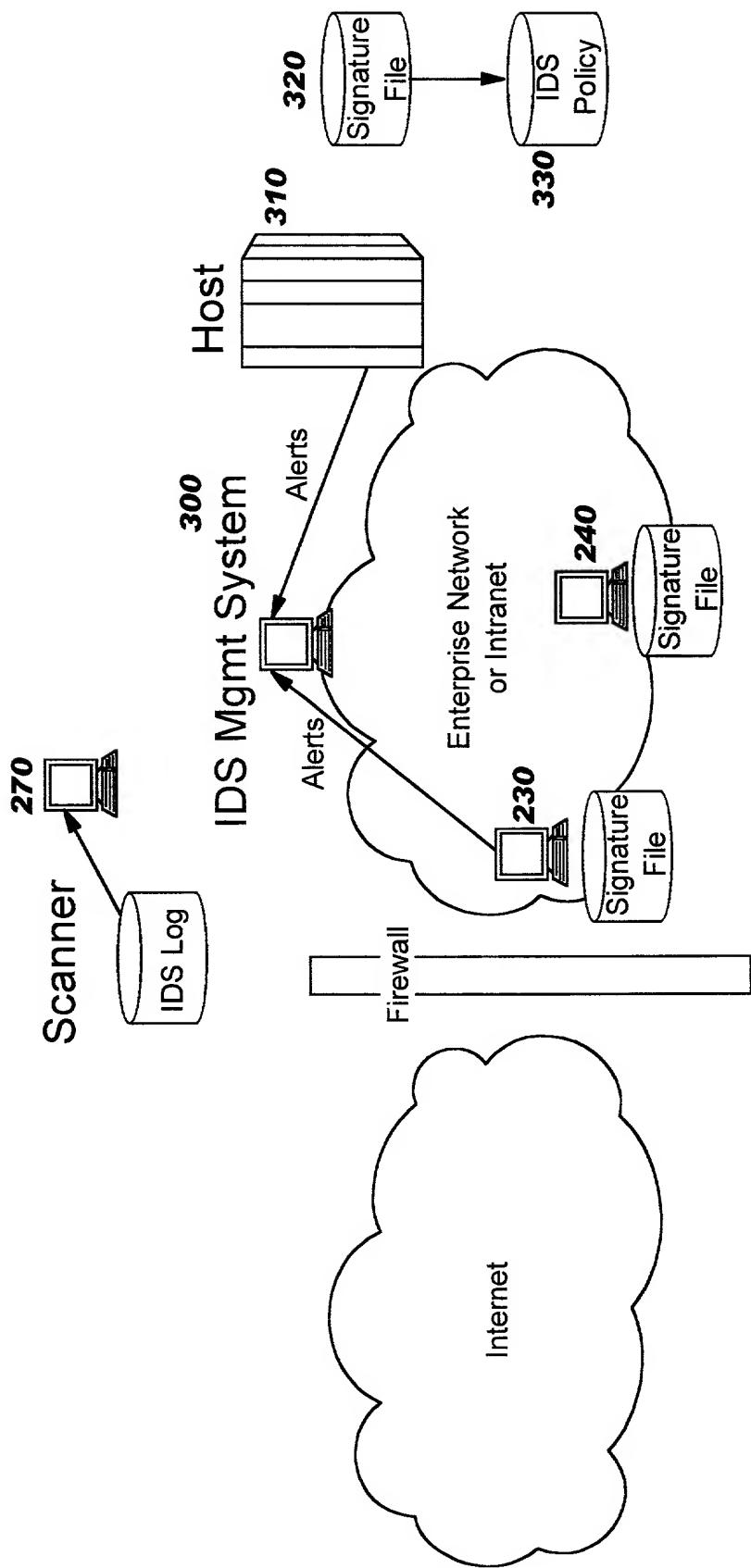


FIG. 4

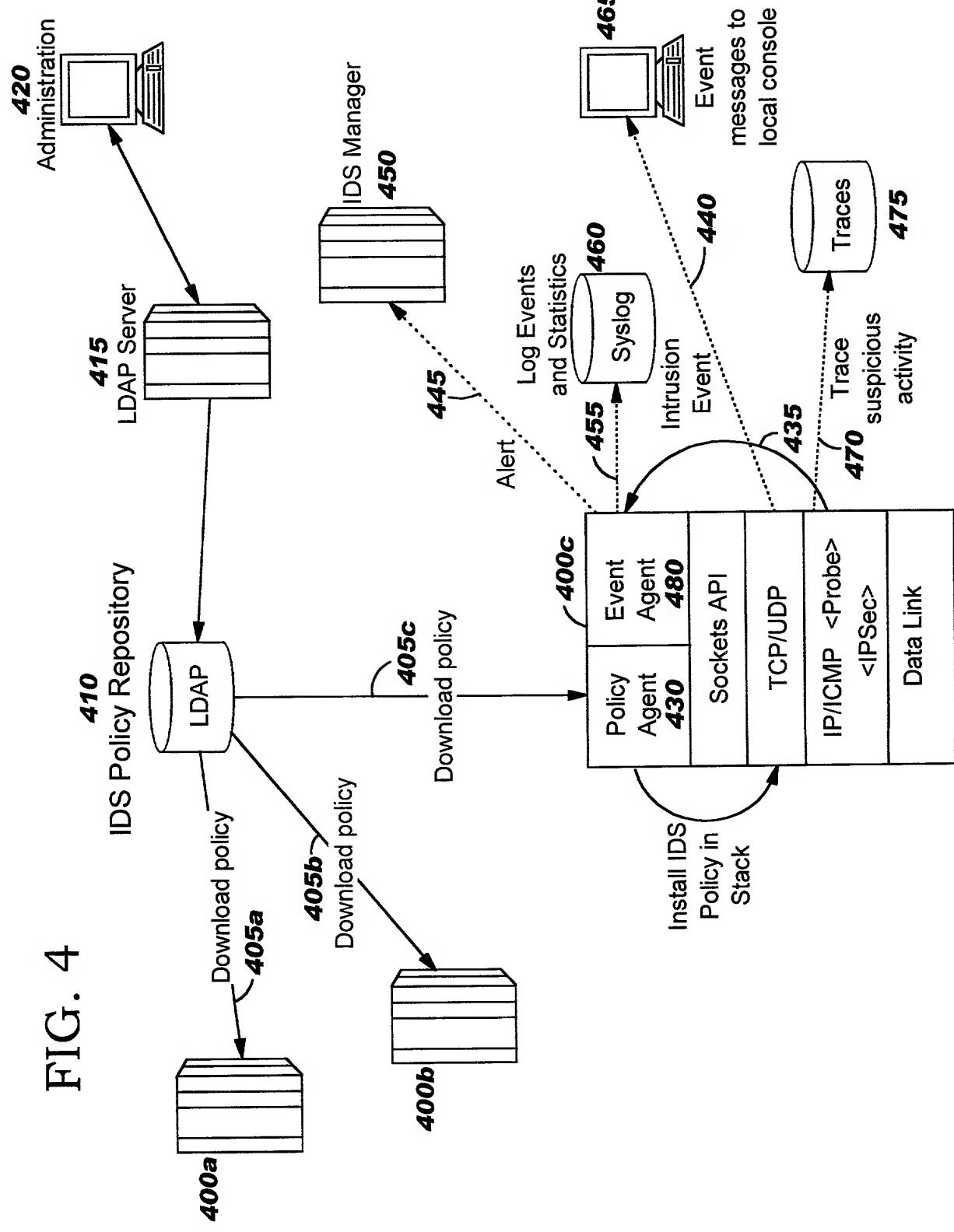


FIG. 5

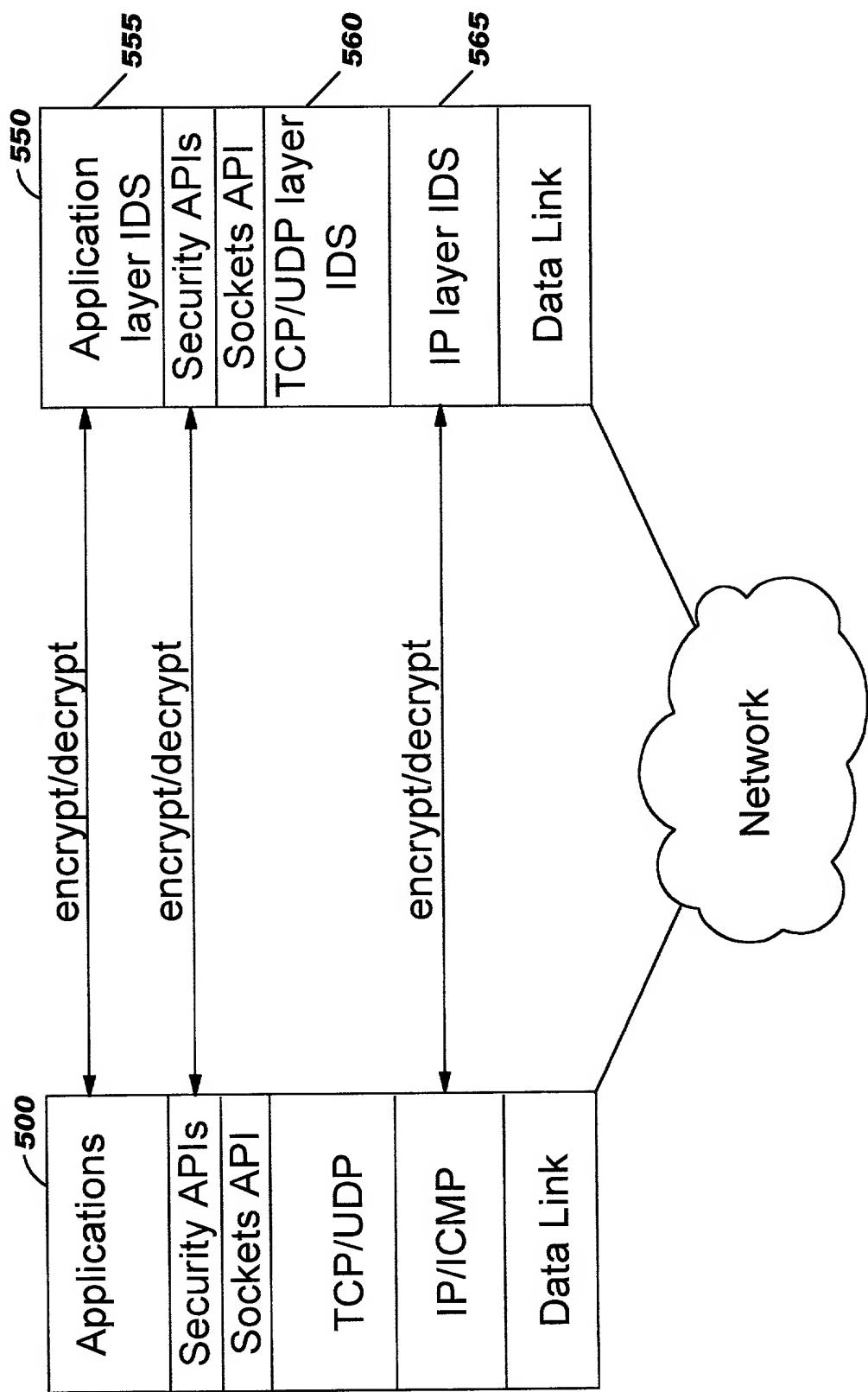


FIG. 6

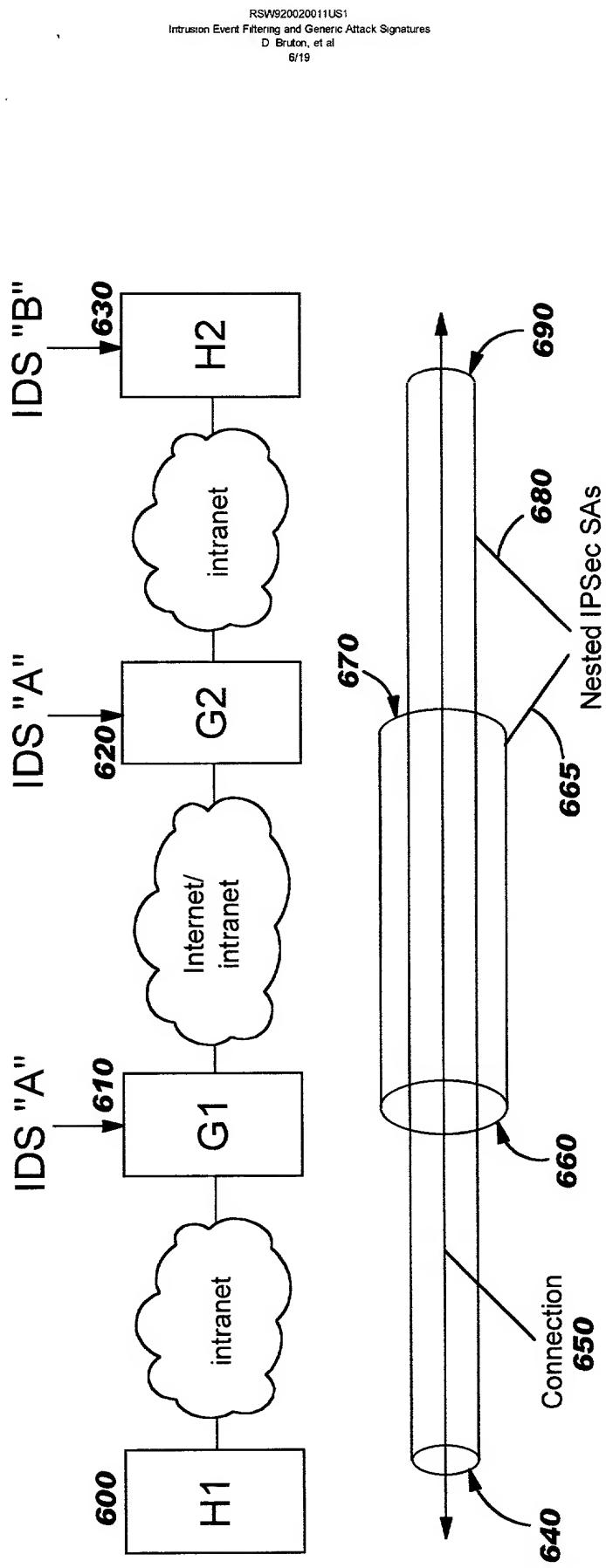


FIG. 7  
(Prior Art)

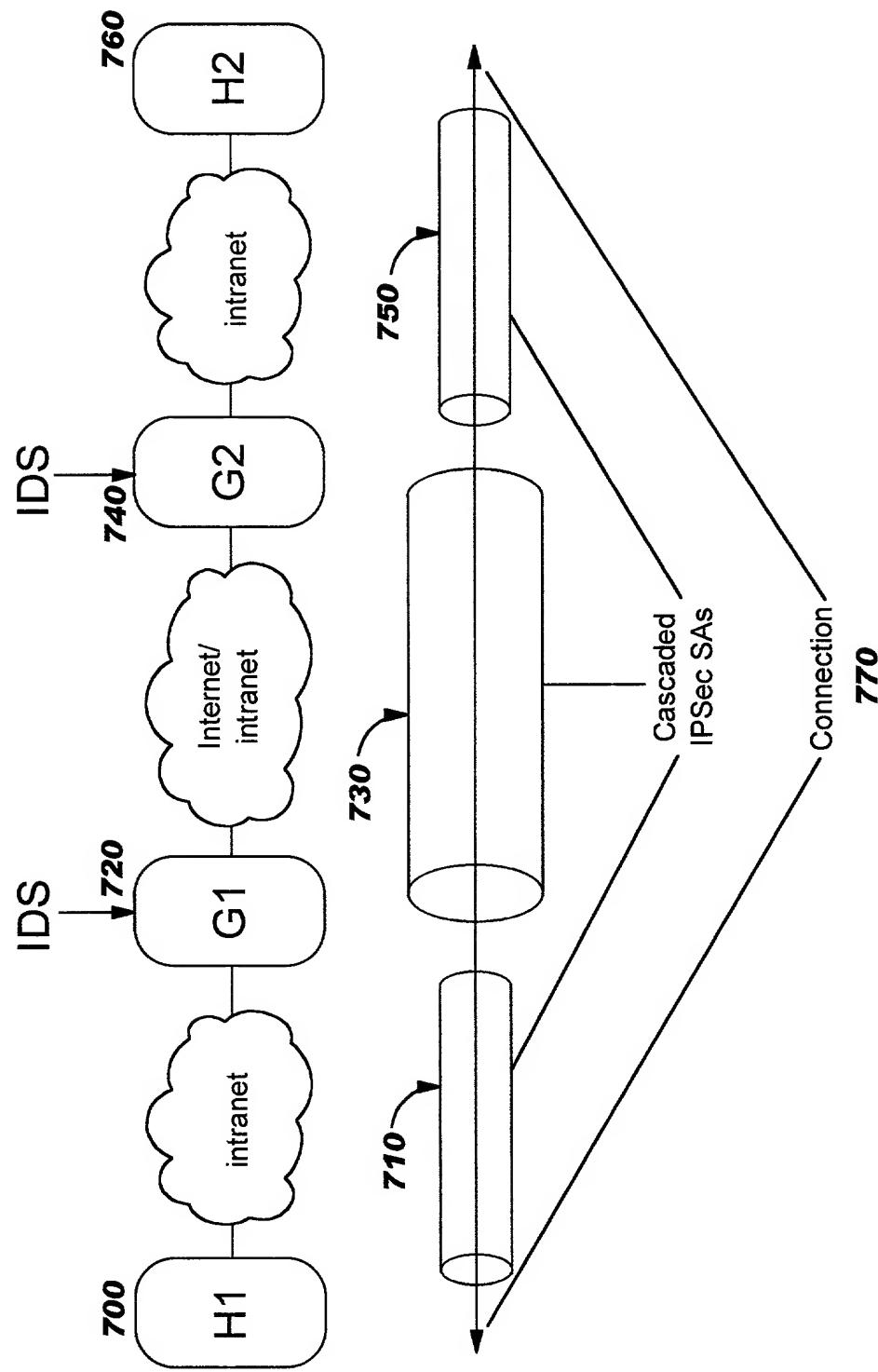


FIG. 8  
(Prior Art)

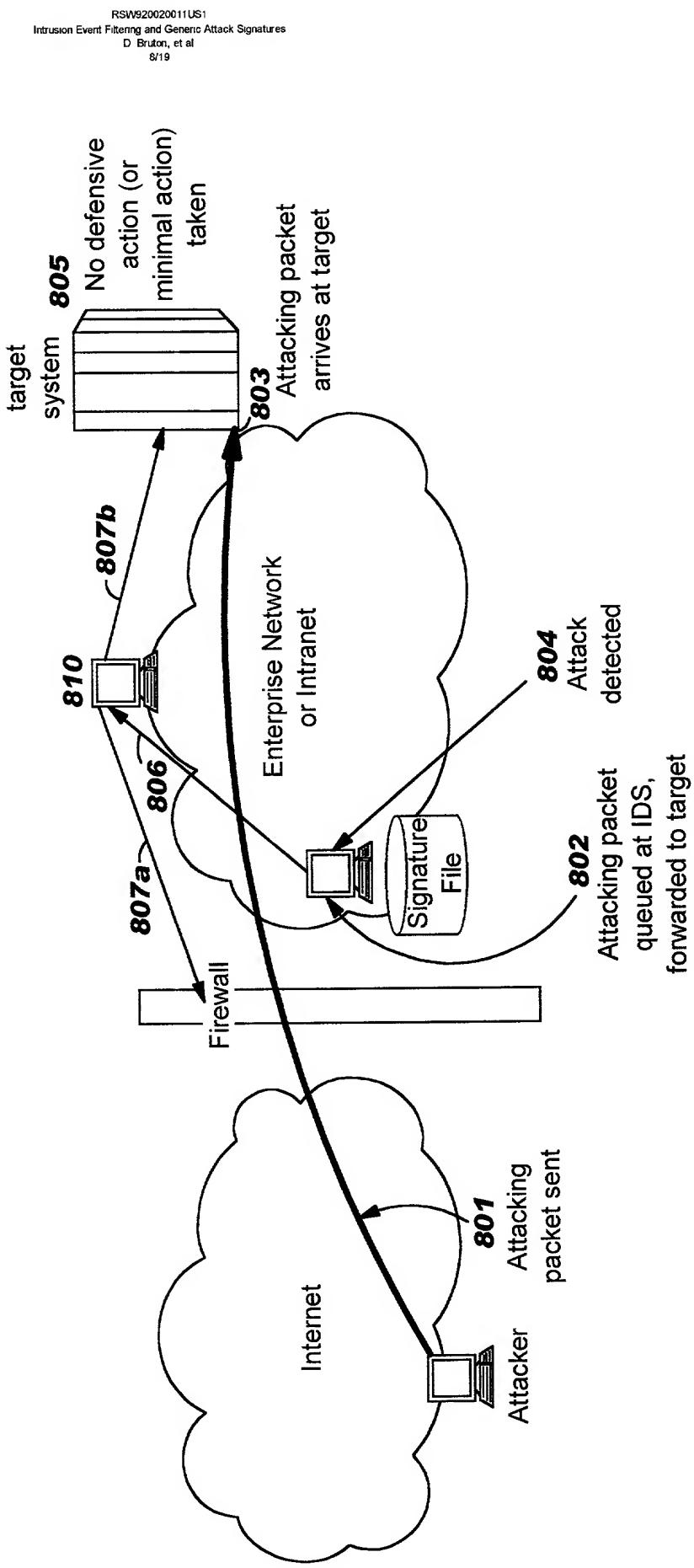


FIG. 9  
IDS Mgmt System

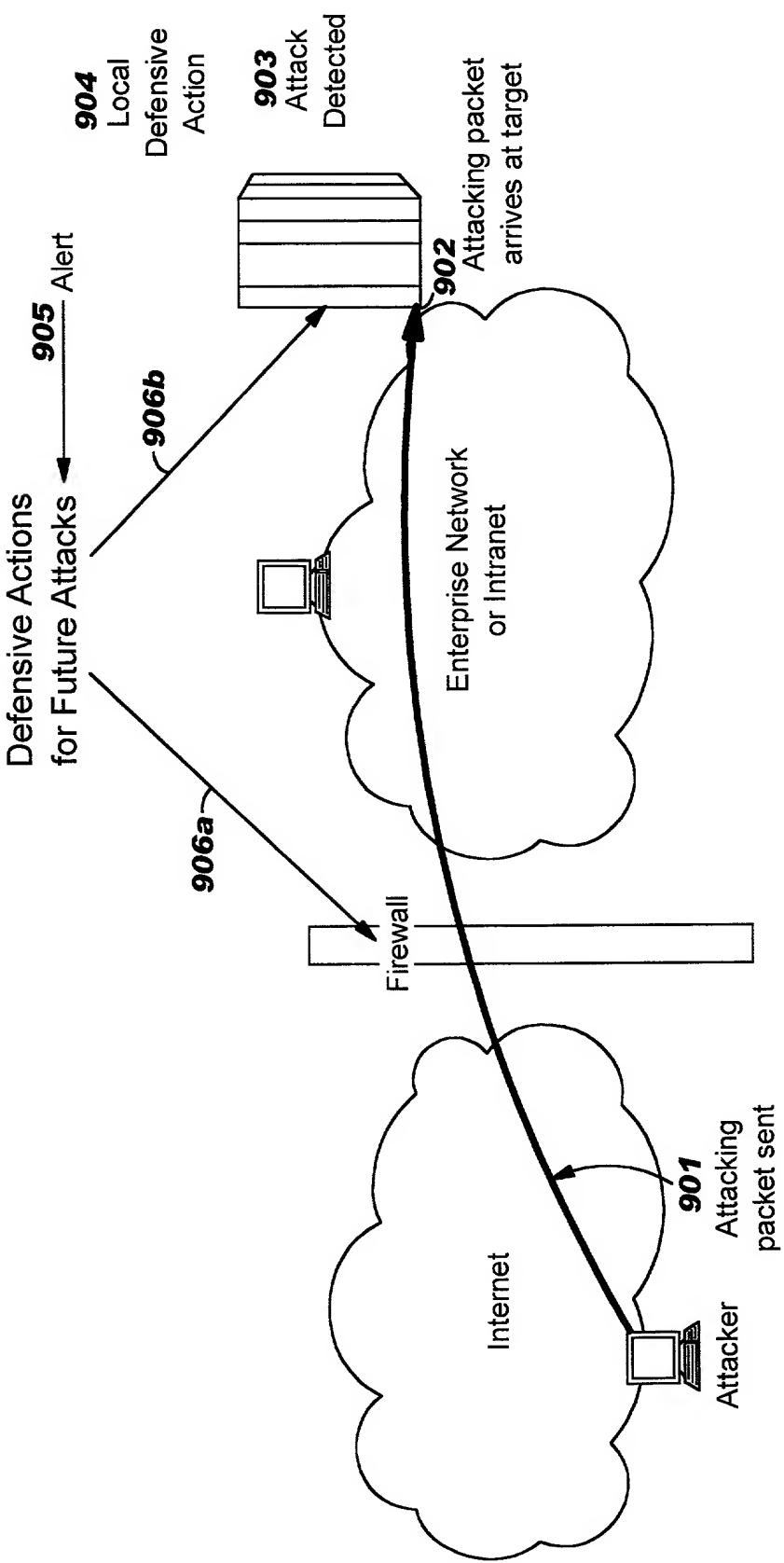


FIG. 10

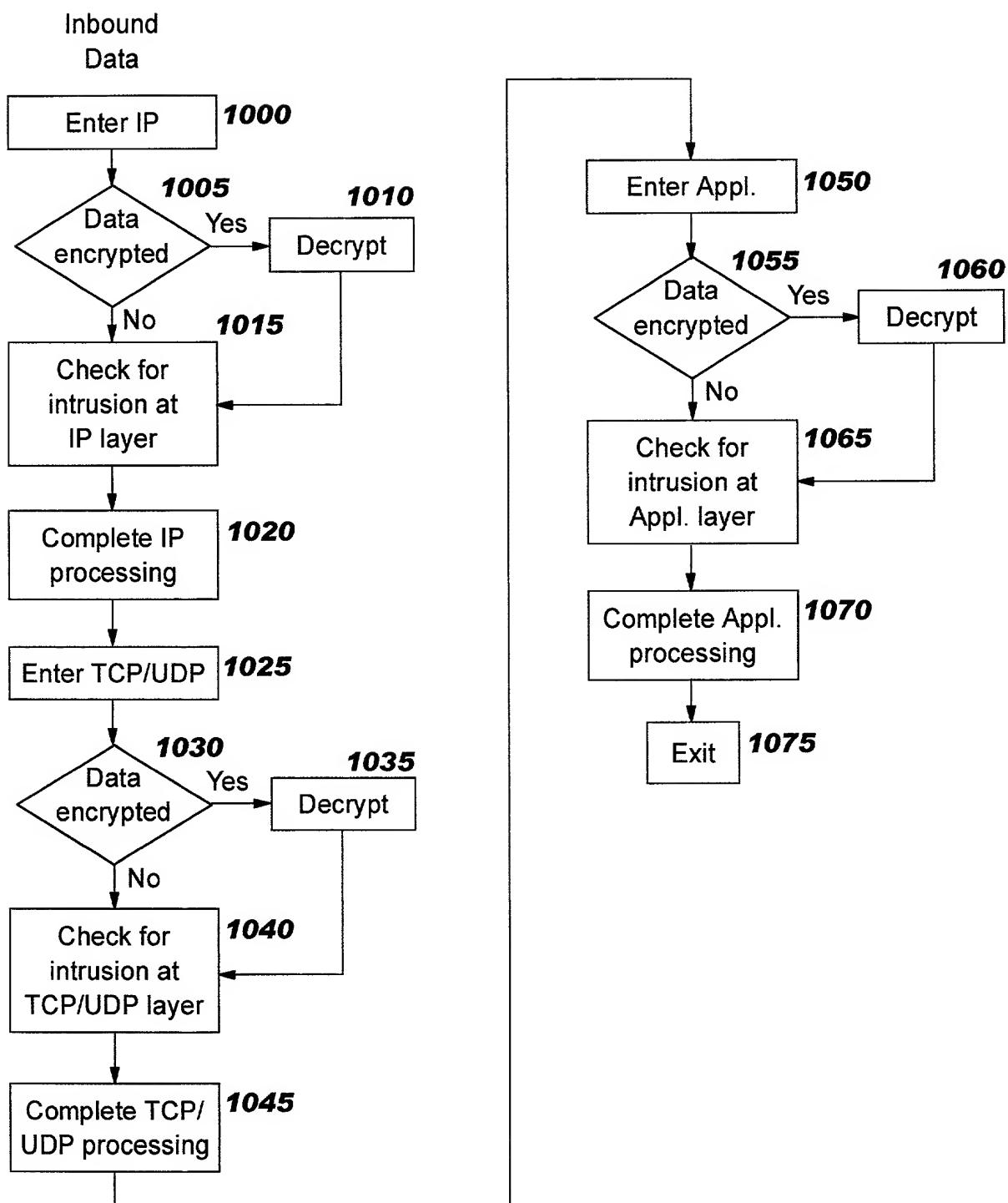
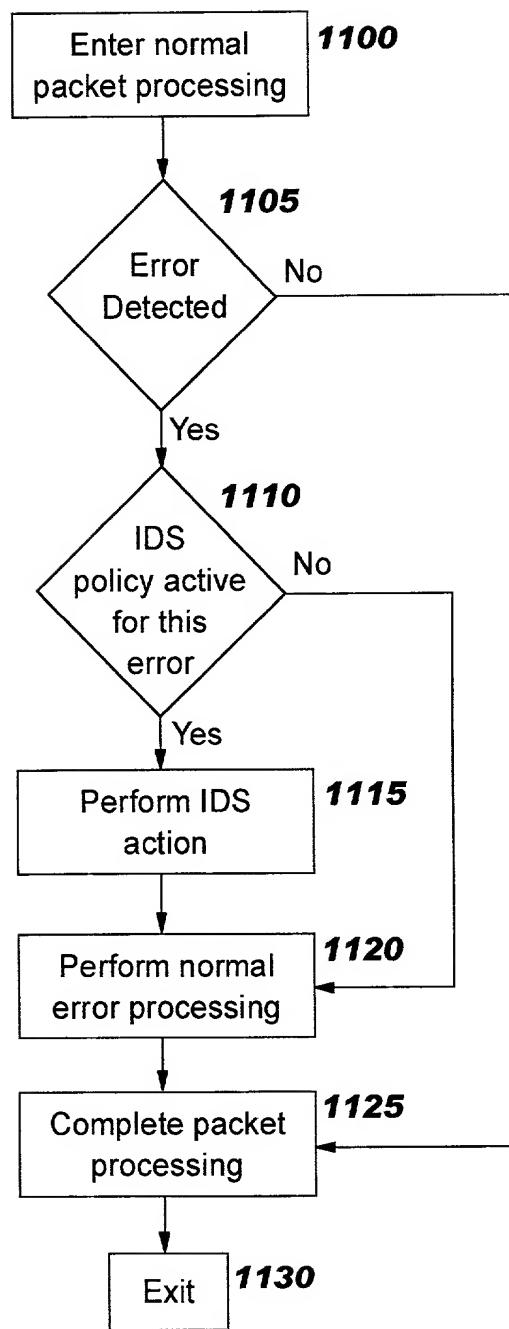


FIG. 11



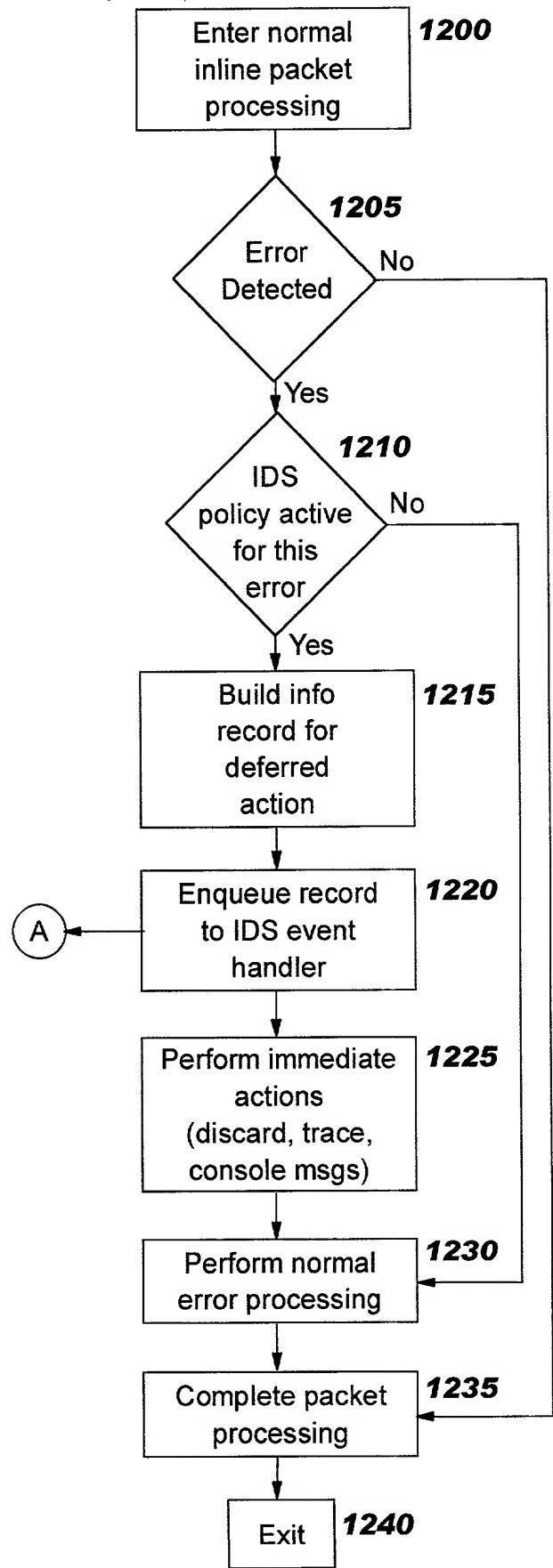


FIG. 12

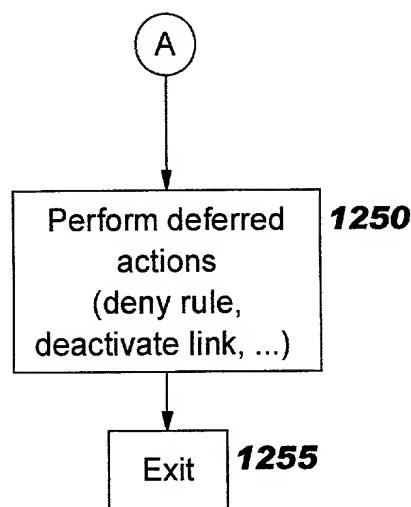


FIG. 13

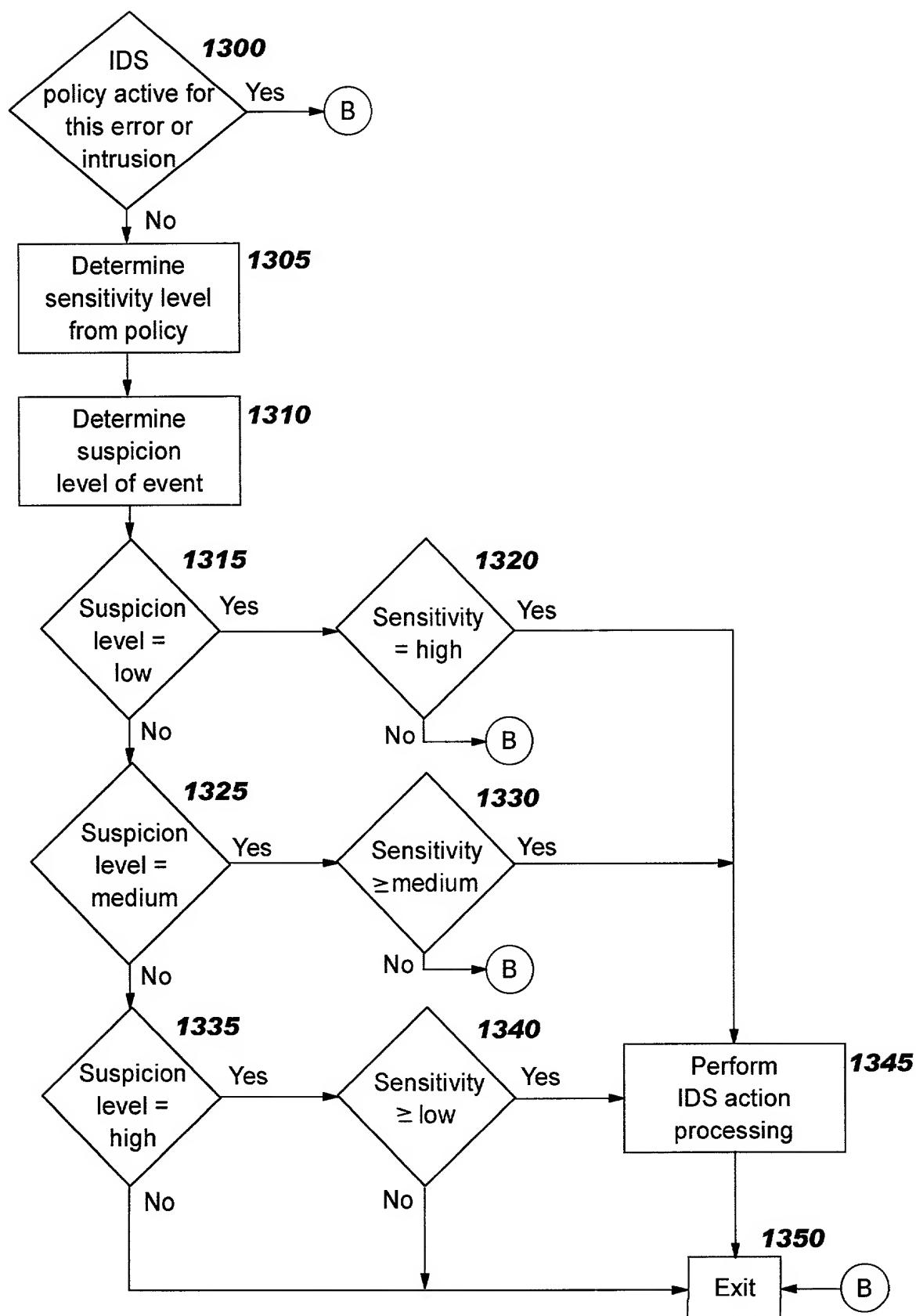


FIG. 14

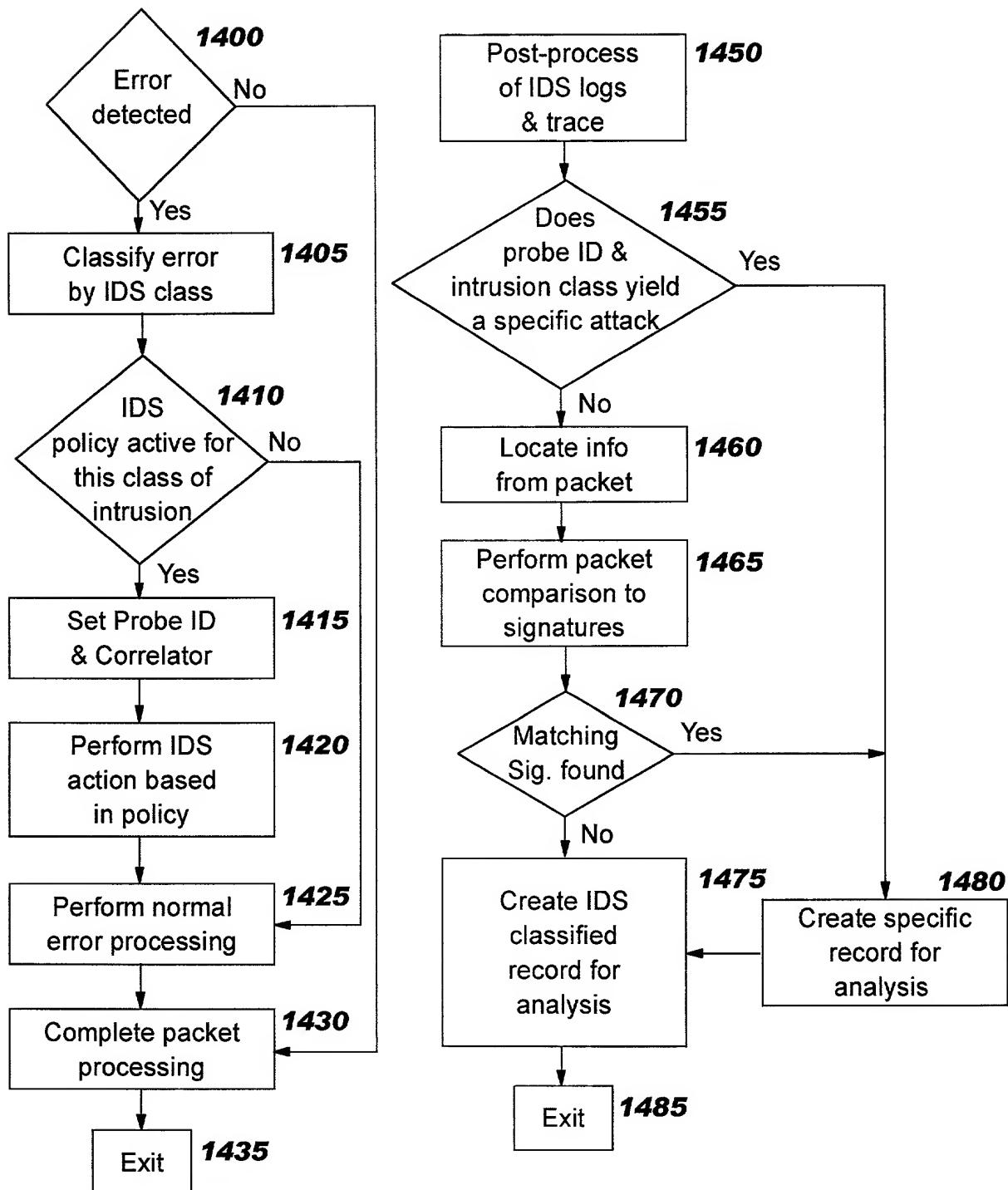


FIG. 15

**1500**

Sensitivity (from policy)	Low Suspicion Event (LS)	Medium Suspicion Event (MS)	High Suspicion Event (HS)
Low			Count
Medium		Count	Count
High	Count	Count	Count

1510      1520      1530

FIG. 16

Basic Policy Objects

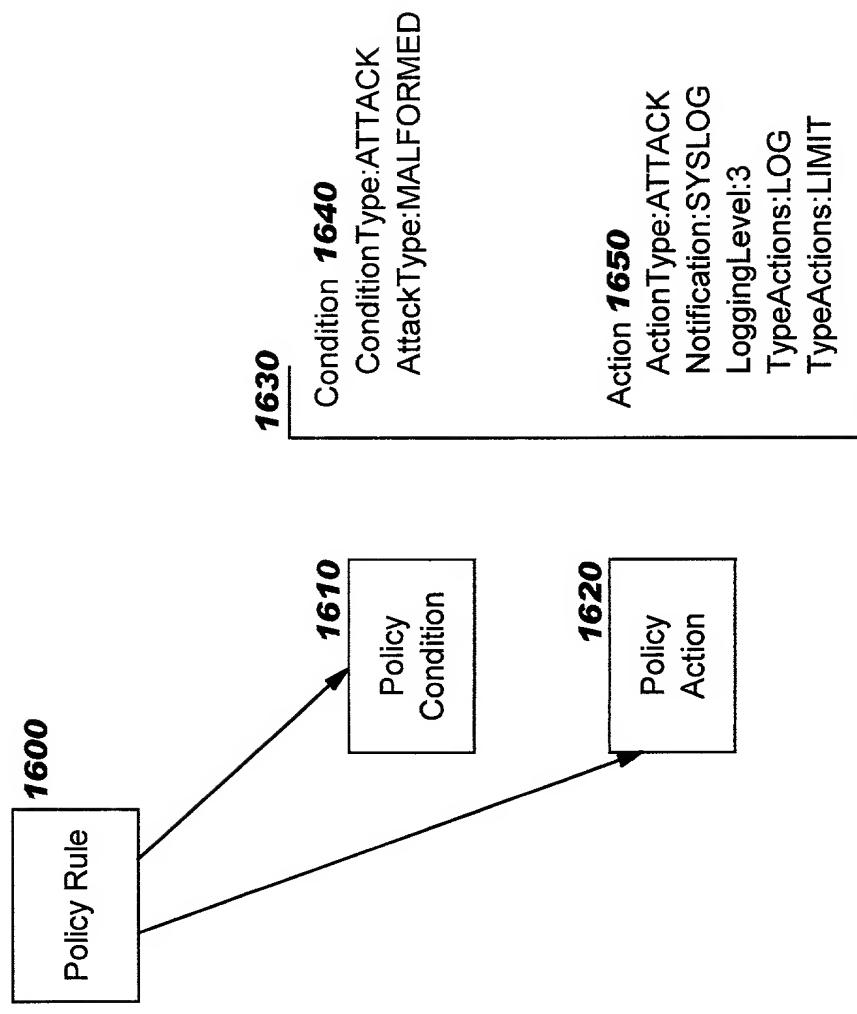


FIG. 17

Socket State	Event	Event Classification
Any state	recv unexpected flags (SYN+FIN...)	high suspicion
RESERVED	recv any packet	high suspicion
Unbound, not RESERVED	recv any packet	medium suspicion - app may be temporarily down
Listen	recv SYN	classification deferred if syn queued.
Half open connection	recv ACK	low suspicion - connection handshake completed
Half open connection	recv RST	medium suspicion - scanner covering tracks?
Half open connection	final time-out (and not syn flood)	high suspicion - scanner abandoning handshake?
Any connected state	seq# out of window	low suspicion - perhaps duplicate packet
Any connected state	recv standalone SYN	low suspicion - perhaps peer reboot
Any connected state	final time-out	medium suspicion - peer abandoned connection

1700

1710 1720 1730

1740

1750

Policy Sensitivity and Event  
 Suspicion Levels for  
 TCP Port Scan

FIG. 18  
IDS Policy Sensitivity and Event Suspicion Levels

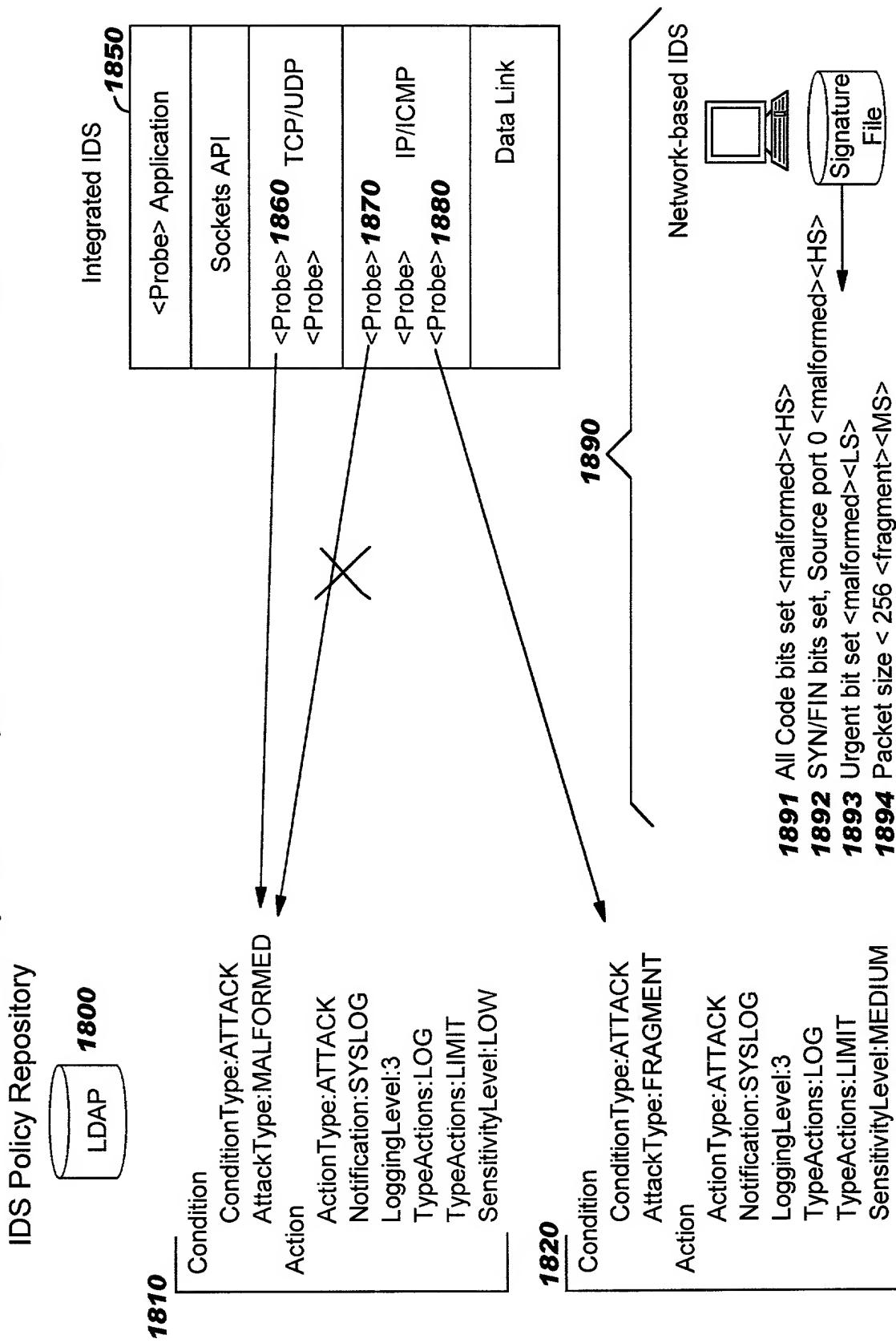


FIG. 19  
Conditions and Actions - Relationship to specific attacks

